IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Atty. Dkt.: 2789-17

Assistant Commissioner for Patents
Washington, D.C. 20231

Date: June 21, 2000

Attached for filing is the patent application of:
Inventor: MÖLLER et al.
Entitled: **DEVICE FOR PROCESSING DATA AND**
CORRESPONDING METHOD

and including attachments as noted below:

☒ Declaration, ☒ Abstract
16 ‥pages of specification and claims (including 30 numbered claims), and
6 sheets of accompanying drawing/s.
☒ Record & return the attached assignment to the undersigned.
☒ Priority is hereby claimed under 35 USC 119 based on the following foreign applications, the entire content of which is hereby incorporated by reference in this application:

Application Number	Country	Day/Month/Year Filed
99 111 962.9	EP	June 25, 1999

, respectively.

☐ Certified copy(ies) of foreign application(s) is/are attached.
☐ Please amend the specification by inserting before the first line --This is a   of PCT application   , filed   , the entire content of which is hereby incorporated by reference in this application.--
☐ Priority is hereby claimed under 35 USC 120/365 based on the following prior PCT applications designating the U.S., the entire content of which is hereby incorporated by reference in this application:

Application Number	Country	Day/Month/Year Filed

☐ This application is based on the following prior provisional application(s):

Application No.	Filing Date

respectively, the entire content of which is hereby incorporated by reference in this application, and priority is hereby claimed therefrom.
☐ Please amend the specification by inserting before the first line: -- This application claims the benefit of U.S. Provisional Application No.   , filed   , the entire content of which is hereby incorporated by reference in this application.
☐ Verified Statement attached establishing "small entity" status (Rules 9 & 27)
☐ The Examiner's attention is directed to the prior art cited in the parent application by applicant and/or Examiner for the reasons stated therein.
☒ Preliminary amendment to claims (attached hereto), to be entered before calculation of the fee below.
☐ Also attached:

FILING FEE IS BASED ON CLAIMS AS FILED LESS ANY HEREWITH CANCELED

Basic Filing Fee						$	690.00
Total effective claims	30	- 20 (at least 20) =	10	x $ 18.00		$	180.00
Independent claims	2	- 3 (at least 3) =	0	x $ 78.00		$	0.00
If any proper multiple dependent claims now added for first time, add $260.00 (ignore improper)						$	0.00
					SUBTOTAL $		870.00
						-$(	0.00)
If "small entity," then enter half (1/2) of subtotal and subtract					SECOND SUBTOTAL $		870.00
						$	40.00
Assignment Recording Fee ($40.00)					TOTAL FEE ENCLOSED $		910.00

Any future submission requiring an extension of time is hereby stated to include a petition for such time extension. The Commissioner is hereby authorized to charge any <u>deficiency</u> in the fee(s) filed, or asserted to be filed, or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our **Account No. 14-1140.** A <u>duplicate</u> copy of this sheet is attached.

1100 North Glebe Road, 8th Floor
Arlington, Virginia 22201-4714
Telephone: (703) 816-4000
Facsimile: (703) 816-4100
JRL:MM

NIXON & VANDERHYE P.C.
By Atty: John R. Lastova, Reg. No. 33,149

Signature: _____

436975

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

MÖLLER et al.   Atty. Ref.: **2789-17**

Serial No.   Group:

Filed: **June 21, 2000**   Examiner:

For: **DEVICE FOR PROCESSING DATA AND
      CORRESPONDING METHOD**

June 21, 2000

Assistant Commissioner for Patents
Washington, DC 20231

PRELIMINARY AMENDMENT

Sir:

Prior to calculation of the filing fee and examination the merits, please amend the above-identified application as follows:

IN THE ABSTRACT:

Please substitute the attached Abstract for the originally filed Abstract.

IN THEN CLAIMS:

Please amend claims 1, 2, 3, 4, 6, 7, 8, 10, 11, 12, 13, 14, 17, 19, 22, 23, 26, 27, 28, and 30 as follows:

1. *(Amended)* Device for processing data, comprising:

a processor [(1)]] for executing program routines, and

a memory [(2)] for storing program routines to be executed by said processor [(1)], where

at least a part of said memory [(2)] is arranged as a protected part [(21)] from which data can be read but which is protected against being written into, and

said processor [(1)] is arranged to necessarily execute a program routine stored in said protected part of said memory upon start-up.

2. *(Amended)* Device according to claim 1, wherein said processor [(1)] stores permanent start addresses [(11)] that are necessarily called upon start-up of said processor [(1)], where at least one of said start addresses points to said protected part [(21)] of said memory [(2)].

3. *(Amended)* Device according to claim 1 [one of claims 1 or 2], wherein said protected part [(21)] of said memory [(2)] is a first part, and said memory further comprises a second part [(22)] into which data can be written, where the program routine from said protected part [(21)] executed by said processor [(1)] upon start-up comprises checking for changes in at least a part of the data contained in said second part [(22)]

4. *(Amended)* Device according to claim 3, wherein said program routine from said protected part [(21)] executed by said processor [(1)] upon start-up comprises calculating a characteristic parameter for data being checked for changes, and comparing said characteristic parameter with a value stored in said second part [(22)] of said memory [(2)] at the time of writing said data being checked for changes into said second part [(22)] of said memory [(2)].

6. *(Amended)* Device according to claim 1 [one of claims 1 to 5], wherein said memory [(2)] comprises a plurality of memory devices [(201, 202, 203)], one [(201)] of which comprises said protected part, and the rest [(202, 203)] of which are arranged such that data may be written into them.

7. *(Amended)* Device according to claim 1 [one of the preceding claims], wherein said protected area [(21)] is arranged such that a mechanism is provided such that after data is initially stored in said protected part [(21)], any subsequent writing of data into said protected part [(21)] is blocked.

8. *(Amended)* Device according to claim 7, wherein said protected area [(21)] is arranged such that the process for storing data therein comprises:

436954

writing [(Si)] data into said protected part [(21)] via a write line, and

sending [(S2)] a signal to said protected part in response to which said write line is

permanently interrupted.

10. *(Amended)* Device according to <u>claim 1</u> [one of claims 1 to 7], wherein said

memory [(1)] comprises a finite state machine, said finite state machine defining a state

which protects said protected part from being written into.

11. *(Amended)* Device according to <u>claim 1</u> [one of the preceding claims], wherein

said memory [(2)] comprise one or more of an EEPROM, a flash memory device, and a

flash memory device emulating an EEPROM.

12. *(Amended)* Device according to <u>claim 1</u> [one of the preceding claims], wherein

said memory [(2)] comprises a memory chip [(5)] having electrical contacts [(51)] for being

connected with a circuit board [(6)] that are arranged such that said electrical contacts [(51)]

are covered by said memory chip [(5)] when said memory chip [(5)] is mounted on said

circuit board [(6)].

13. *(Amended)* Device according to claim 12, wherein said electrical contacts [(51)]

are provided in a ball-grid-array.

14. *(Amended)* Communication device comprising a device for processing data

according to <u>claim 1</u> [one of claims 1 to 13].

17. *(Amended)* Method for controlling a data processing device having a processor

[(1)] for executing program routines and a memory [(2)] for storing program routines to be

executed by said processor [(1)], where at least a part of said memory [(2)] is arranged as a

protected part [(21)] from which data can be read but which is protected against being

written into, comprising:

letting [(S4)] said processor [(1)] necessarily execute a program routine stored in said

protected part of said memory upon start-up [(53)].

- 3 -

19. *(Amended)* Method according to <u>claim 1</u> [one of claims 17 or 18], wherein said protected part of said memory is a first part, and said memory further comprises a second part into which data can be written, where the program routine from said protected part executed by said processor upon start-up comprises checking for changes in at least a part of the data contained in said second part.

22. *(Amended)* Method according to <u>claim 1</u> [one of claims 17 to 21], wherein said memory comprises a plurality of memory devices, one of which comprises said protected part, and the rest of which are arranged such that data may be written into them.

23. *(Amended)* Method according to <u>claim 1</u> [one of claims 17 to 22], wherein said protected area is arranged such that a mechanism is provided such that after data is initially stored in said protected part, any subsequent writing of data into said protected part may be blocked.

26. *(Amended)* Method according to <u>claim 17</u> [one of claims 17 to 23], wherein said memory [(1)] comprises a finite state machine, said finite state machine defining a state which protects said protected part from being written into.

27. *(Amended)* Method according to <u>claim 17</u> [one of claims 17 to 26], wherein said memory comprise one or more of an EEPROM, a flash memory device, and a flash memory device emulating an EEPROM.

28. *(Amended)* Method according to <u>claim 17</u> [one of claims 17 to 27], wherein said memory comprises a memory chip having electrical contacts for being connected with a circuit board that are arranged such that said electrical contacts are covered by said memory chip when said memory chip is mounted on said circuit board.

30. *(Amended)* A medium readable by a data processing device, having a program recorded thereon, where the program is to make the data processing device execute the method of <u>claim 17</u> [one of claims 17 to 29].

436954

REMARKS

By the foregoing amendment, Applicants have amended claims 3, 6, 7, 10, 11, 12, 14, 19, 22, 23, 26, 27, 28, and 30 to eliminate the multiple claim dependencies in order to minimize the filing fee. The claims have also been amended to eliminate the parentheticals appearing in the claims to conform to U.S. practice.

Prompt and favorable examination on the merits is respectfully requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____

John R. Lastova
Reg. No. 33,149

JRL:mm
1100 North Glebe Road, 8th Floor
Arlington, VA 22201-4714
Telephone: (703) 816-4000
Facsimile: (703) 816-4100

Attachment: Abstract

- 5 -

436954

ABSTRACT

Device for processing data includes a processor for executing program routines, and a memory for storing program routines to be executed by the processor. Part of the memory includes a protected part from which data can be read but which is protected against being written into. The processor is arranged to necessarily execute a program routine stored in the protected part of the memory upon start-up.

U.S. PATENT APPLICATION

Inventors: **Bernd MÖLLER**
                Harro OSTHOFF
                Ben SMEETS
                Kar-Fat POON

Invention: **DEVICE FOR PROCESSING DATA AND CORRESPONDING METHOD**

SPECIFICATION

Device for processing data and corresponding method

Field of the invention

The present invention relates to a device for processing data and a method for controlling such a device.

Background of the invention

The use of data processing systems comprising processing elements and memory elements have become widespread in very different fields of electronics. In the field of communication, most communication devices contain processors that execute programs stored in appropriate memory devices, to thereby process data stored in the same memory devices or somewhere else. A typical example of a communication device containing a processor (typically a microprocessor controller) and appropriate memory chips is a mobile telephone.

One of the problems encountered with data processing systems is that of data security. For example, the above-mentioned mobile phone may contain different types of memories separated from the central processor, such as a flash memory or an EEPROM. It is possible that an EEPROM is emulated by a flash memory or is partly a flash memory. Such memories typically have to be protected against unauthorized access, in order to safeguard the normal operation of the mobile telephone.

Naturally, the problem of data security occurs in any such data processing system, not only in mobile phones. The basic solution to problems of data security is the provision of protection software, e.g. an algorithm for the authentication

of sensitive data in the EEPROM or emulated EEPROM. However, such software solutions suffer from a number of problems that cannot be overcome by software itself, such as the possibility of switching off the authentication algorithm or modifying the authentication algorithm. Sometimes, it is also possible to circumvent an authentication algorithm by using older software that did not contain the authentication routine but still provides access to the sensitive data.

Summary of the invention

The object of the present invention is to provide a better device for data processing, which is fairly simple to implement and solves the above problems.

This object is achieved by the device described in claim 1 and the method described in claim 14.

In accordance with the present invention, in a data processing device having a memory means and a processing means, there is provided on the one hand a protected section in the memory means of a data processing device, and on the other hand the processing means in is arranged to necessarily execute a program routine stored in the protected part of the memory upon start-up. Due to this arrangement, specific programs that are e.g. associated with security can be executed, where an unauthorized person is prevented from performing changes in said programs, because they are stored in a protected part of the memory. Such security programs can e.g. be programs that establish that other data has not been tampered with, as shall be explained in more detail further on.

An important aspect of the present invention is the fact that no modification of the processor is necessary. In other words, the straightforward solution to the above-mentioned problems would have consisted in modifying the processing

means to thereby contain security mechanisms, but such a modification of a processor is typically complicated, time consuming and costly. In contrast thereto, the present invention provides a very simple arrangement, in which only a modified memory is necessary, which is far simpler. Especially, processors already in use may be retained, in which case the memories have to be arranged in such a way that the addresses fixed in said processors for start-up (so-called start addresses) point to the protected section of the memory devices. As an alternative, a slight modification of the processors could be performed, namely changing the start addresses. Although this is a modification of the processor, it is fairly simple and not costly.

Preferred embodiments of the invention are described in the dependent claims.

Brief description of drawings

The various advantages and features of the present invention will become more apparent by studying the following detailed description of embodiments of the invention, where said description makes reference to the figures, in which:

Fig. 1   shows a basic arrangement of an embodiment of the present invention;

Fig. 2   shows an arrangement of another embodiment of the present invention;

Figs. 3a and 3b
            show a preferred memory device to be used in the data processing device of the present invention;

Fig. 4   shows a flow-chart of a process for storing data in the protected part and subsequently protecting said data;

Fig. 5   is a flow-chart explaining the basic operation of the data processing device of the present invention; and

Fig. 6   is a schematic diagram of an embodiment of a memory means.

Detailed description of embodiments

Fig. 1 shows an embodiment of the present invention. Reference numeral 1 refers to a processor, such as a microprocessor controller. Reference numeral 11 symbolizes start addresses in said processor, where said start addresses are implemented in such a way that they cannot be changed from the outside. In other words, the processor 1 is arranged in such a way that it necessarily calls the start-addresses stored in section 11 when the processor is started.

Reference numeral 2 is a memory system comprising a first section 21, which is a protected section, and a second section 22, in which data may freely be written. The processor 1 and memory 2 are connected by address lines 3 and data lines 4, and CLK symbolizes that the circuits are supplied with a clock signal, while U symbolizes that the circuits are supplied with an operating voltage.

The protected section is protected against data being written into it. This may be accomplished in any way suitable or desirable for the application at hand.

The protected section 21 is preferably arranged in such a way that it is not at all possible to write data into said section after an initial storing of data in said section has taken place. In other words, the memory must be arranged in such a way that specific data or program routines can be stored in the protected section 21 initially, and then a

mechanism must be used for ensuring that no subsequent writing of data into said section is possible. One preferred embodiment of a memory accomplishes this in a way shown in Fig. 4. In this case, a so-called one-time programming area is provided in a flash memory device, where this flash memory device incorporates a mechanism for making a write line to the protected section impassable (e.g. destroying the write line by burning it through, so-called fusable link). The destruction of the write line is performed by the memory in response to a predetermined signal. In this way, the necessary programs and data can be written into the protected section (step S1 in Fig. 4) by the manufacturer of the apparatus into which the data processing device of the invention is to be built-in (i.e. the manufacturer of mobile telephones), after which the predetermined signal is sent to thereby burn-through the write line (fusable link). As a consequence, no subsequent writing of data into the protected section is possible, such that the data in said section cannot be changed. (Step S2 in Fig. 4).

Naturally, this is only a preferred example, and the present invention extends to any type of memory device, in which it is possible to protect a specified part of the memory from write access. As an example, memories are known, in which a certain number of input lines are given, where a predetermined part of the memory is protected from write access as long as certain predetermined signals (such as a ground voltage 0 or a supply voltage) are present on the input lines.

Another example will be explained in connection with Fig. 6, which shows a memory with a so-called finite state machine FS. Finite state machines are known in the art, and will therefore only briefly be described here. The depicted memory 1A has an address bus 70, a data bus 71, read/write (R/W) access line 72, and a line 73 for switching the states of the finite state machine (FS). NO symbolizes normal operation,

and FSO symbolizes finite state operation. The finite state machine is basically a program that is hard-wired into the memory 1A, such that it cannot be changed from the outside, thereby fulfilling basic security requirements. This hard-wired program is part of the address logic that processes the addresses sent to the memory over the address bus.

As an example, if line 73 is high (i.e. 1), then the memory is in a normal state of operation and the data bus 71 is used in the normal fashion for transporting data. If line 73 is low (i.e. 0), then the data bus is used for controlling the finite state machine FS.

In the application to the present invention, the finite state machine will have two states, namely a first state in which it is allowed to write data into a predetermined section of the memory 1A (i.e. this section will be the protected section), and a second state, which is a locked state, in which writing into the predetermined section is disabled. The finite state machine is arranged such that the transition from the first state to the second state is irreversible, i.e. once the machine is locked, it is no longer possible to switch back to the first state, and therefore it is no longer possible to write into the protected section. This can be done in any suitable way with known finite state machines, for example by selecting the finite state program such that the locked state depends on a specific value in the protected section, such that as long as the initial value is at the specific address a writing into the protected section is allowed, whereas once the value at the specific address has changed (this is the state transition), the finite state program will go into an endless loop or terminate if an attempt is made to write into an address in the protected section, and because the specific address is in the protected section, it may not be changed, so that the locked state is permanent.

Returning now to Fig. 1, the system is arranged in such a way that the addresses contained in section 11 of processor 1 point towards the protected section 21 in memory 2. In other words, upon start-up, the processor 1 will call one or more addresses in the protected part 21 of memory 2, and consequently execute the programs contained therein. This is explained in the top-part of Fig. 5, which shows a flow chart of the control operation in accordance with the present invention. In a first step S3, the memory and processor CP are started by supplying voltage U and a clock signal CLK. Then, in step S4, the processor CP calls the start addresses that point to the protected part of the memory. Finally, in step S5, the processor CP executes the programs from the protected part.

It may be noted that it is not necessary for specific programs to be stored in the protected part 21 of memory 2, because in the event of the processor 1 already being programmed, it may be sufficient that the processor only calls up specific parameters stored in the protected section 21, where these parameters are then processed by the processor 1 in the preprogrammed routines.

The precise processing conducted upon start-up can be selected in accordance with the specific requirements and desires of the given application. In accordance with a preferred embodiment, the routines carried-out upon start-up are security routines, for example shown in the bottom part of the flow-chart in Fig. 5. More specifically, in the case of Fig. 5, the program routine executed upon start-up checks for unauthorized changes of data in the unprotected section 22 of memory 2.

As an example, in the event that the data processing device of the present invention is employed in a mobile telephone, then certain parameters associated with the specific user of said mobile telephone (such as service, priorities, etc.) can

be stored in said unprotected section 22, where it is
possible that these parameters are changed during the routine
processing performed by processor 1. However, it will also be
possible that an unauthorized user will access these data and
change them. One possibility of checking for such an
unauthorized access consists in additionally storing a
characterizing parameter for the data in said unprotected
section 22 together with any changed parameters. A typical
example of such a characterizing parameter is the check
sum. Another example is a result of a computation of a
cryptographic hash function. In other words, every time that
the authorized entity (the processor) changes data in section
22, then an accordingly changed check sum is also stored. In
this way, the routine for checking if unauthorized access and
changes have been performed can consist in calculating the
check sum and comparing said check sum to the stored value.
If a discrepancy occurs, then the routine determines that an
unauthorized change of data has taken place. As shown in the
bottom part of Fig. 5, the routine can react to the detection
of an unauthorized change (yes in step S6) by invoking any
sort of desired security or emergency procedure (such as
shutting-off the device), or if no changes are detected,
proceeding with normal operation.

Although the memory 2 shown in Fig. 1 appears as a single
unit, this is to be understood as an abstract description, as
said memory may be a single unit, but can equally well
consist of a plurality of physically separate memory-devices,
as e.g. shown in Fig. 2. Fig. 2 uses the same reference
numerals for components already described in connection with
Fig. 1, so that a repeated description is not necessary. As
shown in Fig. 2, memory 2 comprises a plurality of memory
devices, such as individual memory chips 201, 202, 203 .....
The precise arrangement of the memory devices or chips is of
no importance to the present invention. For example, it is
possible that the protective section shown as 21 in fig. 1 is
formed by the entire chip 201 in fig. 2, i.e. this chip 201

is arranged in such a way that there is no write access. Then the remaining chips 202, 203.... could all be conventional EEPROMs, i.e. chips into which normal write access is possible. Naturally, it is equally well possible, that each chip 201, 202, 203, ...has a first section that is protected, and a second section, that is not protected, where for example the addresses in section 11 of processor 1 point to an address in the protected part of chip 201, and this protected part of chip 201 in turn points to other protected parts of the other chips 202, 203, ... In the latter case, all of the protected sections of the chips 210, 202, 203,.... would together constitute the protected part of the memory means described in the claims.

It may be noted, that although the above-described embodiments relate to a system in which the memory has a protected part into which data cannot be written, it is still possible to read out the data in the protected section, even for an unauthorized user. In order to make this more difficult for an unauthorized user, a preferred embodiment of the memory in the data processing device of the present invention is shown in Figs. 3a and 3b. Figs. 3a and 3b show a memory chip 5 having electrical contacts 51 that are to be soldered or otherwise connected to electrical leads 61 on a circuit board 6. Fig. 3a shows the components before mounting and Fig. 3b shows the arrangement after the memory chip 5 has been mounted onto circuit board 6, where the electrical contacts 51 and electrical leads 61 have been unified into contacts 71. It may be noted that the representation of Fig. 3b is exaggerated in the sense that in reality the distance between memory chip 5 and circuit board 6 will be very small, such that there is practically no possibility of accessing the contacts 71 while the chip 5 is mounted on the board 6.

Therefore, as indicated in Fig. 3, the electrical contacts 51 are such that the resulting contacts 71 are completely covered by the chip 5 after said chip has been mounted on the

circuit board, to thereby make it impossible to access the electrical contacts 51 from the outside. For example, the contacts 51 can be small semi-spheres arranged in so-called ball-grid array.

By using the arrangement of Fig. 3, it is possible to avoid that an unauthorized user can pick up the signal passing through the contacts during the operation of the memory chip, such that a monitoring of the signals going in and coming out of the memory chip 5 during operation necessitates dismounting the chip from the circuit board and then providing corresponding replacement connections. This is a complicated and tedious procedure that may be expected to let any prospective unauthorized user shy away from attempting to monitor the signals between the memory and the remaining circuits. It may be noted that even though it is possible to read out data from protected section 21 after having dismounted the memory chip 5 from the circuit board 6, it will nonetheless be a very complicated and tedious procedure to re-mount the chip onto the circuit board, because such mounting procedures are performed by high-precision machines during manufacturing, i.e. the spacing between contacts is typically very small.

Naturally, the connections between the memory and the processor on the circuit board should also be hidden in an appropriate fashion, e.g. in such a way that an attempt to access them requires destroying the circuit board, and the electrical contacts to the processor should also be inaccessible, e.g. with the help of the measures described above in connection with the memory.

As already mentioned, the present invention provides an arrangement in which a fairly high amount of data security can be achieved in an inexpensive way. A preferred application of the data processing device of the invention is in communications devices. Such communications devices can

e.g. be mobile telephones. A specifically preferred application of the data processing device is to communication devices adhering to the so-called Bluetooth technology. Bluetooth technology is designed to enable users to connect their mobile computers, digital cellular phones, handheld devices, network access points and other mobile devices via wireless short-range radio links unimpeded by line-of-sight restrictions. Eliminating the need for proprietary cables or for line-of-sight communication via IR-links to connect devices, Bluetooth technology increases the ease and breadth of wireless connectivity. Bluetooth operates in the 2.45 GHz ISM "free band". Details on this technology may be found e.g. at http://www.bluetooth.com.

The present invention has been described by way of examples, but it shall be understood that these examples only serve to clearly present the invention to a skilled person and do not intend to restrict the scope of the invention in any way. Much rather, the scope of the invention is determined by the appended claims.

What is claimed is:

1. Device for processing data, comprising:

    a processor (1) for executing program routines, and

    a memory (2) for storing program routines to be executed
    by said processor (1), where

    at least a part of said memory (2) is arranged as a
    protected part (21) from which data can be read but
    which is protected against being written into, and

    said processor (1) is arranged to necessarily execute a
    program routine stored in said protected part of said
    memory upon start-up.

2. Device according to claim 1, wherein said processor (1)
    stores permanent start addresses (11) that are
    necessarily called upon start-up of said processor (1),
    where at least one of said start addresses points to
    said protected part (21) of said memory (2).

3. Device according to one of claims 1 or 2, wherein said
    protected part (21) of said memory (2) is a first part,
    and said memory further comprises a second part (22)
    into which data can be written, where the program
    routine from said protected part (21) executed by said
    processor (1) upon start-up comprises checking for
    changes in at least a part of the data contained in said
    second part (22).

4. Device according to claim 3, wherein said program
    routine from said protected part (21) executed by said
    processor (1) upon start-up comprises calculating a
    characteristic parameter for data being checked for
    changes, and comparing said characteristic parameter

with a value stored in said second part (22) of said memory (2) at the time of writing said data being checked for changes into said second part (22) of said memory (2).

5. Device according to claim 4, wherein said characteristic parameter is a check sum.

6. Device according to one of claims 1 to 5, wherein said memory (2) comprises a plurality of memory devices (201, 202, 203), one (201) of which comprises said protected part, and the rest (202, 203) of which are arranged such that data may be written into them.

7. Device according to one of the preceding claims, wherein said protected area (21) is arranged such that a mechanism is provided such that after data is initially stored in said protected part (21), any subsequent writing of data into said protected part (21) is blocked.

8. Device according to claim 7, wherein said protected area (21) is arranged such that the process for storing data therein comprises:
writing (S1) data into said protected part (21) via a write line, and
sending (S2) a signal to said protected part in response to which said write line is permanently interrupted.

9. Device according to claim 8, wherein said write line is a fusable link.

10. Device according to one of claims 1 to 7, wherein said memory (1) comprises a finite state machine, said finite state machine defining a state which protects said protected part from being written into.

11. Device according to one of the preceding claims, wherein said memory (2) comprise one or more of an EEPROM, a flash memory device, and a flash memory device emulating an EEPROM.

12. Device according to one of the preceding claims, wherein said memory (2) comprises a memory chip (5) having electrical contacts (51) for being connected with a circuit board (6) that are arranged such that said electrical contacts (51) are covered by said memory chip (5) when said memory chip (5) is mounted on said circuit board (6).

13. Device according to claim 12, wherein said electrical contacts (51) are provided in a ball-grid-array.

14. Communication device comprising a device for processing data according to one of claims 1 to 13.

15. Communication device according to claim 14, wherein said communication device is a mobile telephone.

16. Communication device according to claim 14, wherein said communication device is a bluetooth communication device.

17. Method for controlling a data processing device having a processor (1) for executing program routines and a memory (2) for storing program routines to be executed by said processor (1), where at least a part of said memory (2) is arranged as a protected part (21) from which data can be read but which is protected against being written into, comprising:
letting (S4) said processor (1) necessarily execute a program routine stored in said protected part of said memory upon start-up (S3).

18. Method according to claim 17, wherein said processor stores permanent start addresses that are necessarily called upon start-up of said processor, where at least one of said start addresses points to said protected part of said memory.

19. Method according to one of claims 17 or 18, wherein said protected part of said memory is a first part, and said memory further comprises a second part into which data can be written, where the program routine from said protected part executed by said processor upon start-up comprises checking for changes in at least a part of the data contained in said second part.

20. Method according to claim 19, wherein said program routine from said protected part executed by said processor upon start-up comprises calculating a characteristic parameter for data being checked for changes, and comparing said characteristic parameter with a value stored in said second part of said memory at the time of writing said data being checked for changes into said second part of said memory.

21. Method according to claim 20, wherein said characteristic parameter is a check sum.

22. Method according to one of claims 17 to 21, wherein said memory comprises a plurality of memory devices, one of which comprises said protected part, and the rest of which are arranged such that data may be written into them.

23. Method according to one of claims 17 to 22, wherein said protected area is arranged such that a mechanism is provided such that after data is initially stored in said protected part, any subsequent writing of data into said protected part may be blocked.

24. Method according to claim 23, wherein said protected area is arranged such that the process for storing data therein comprises:

writing data into said protected part via a write line, and

sending a signal to said protected part in response to which said write line is permanently interrupted.

25. Method according to claim 24, wherein said write line is a fusable link.

26. Method according to one of claims 17 to 23, wherein said memory (1) comprises a finite state machine, said finite state machine defining a state which protects said protected part from being written into.

27. Method according to one of claims 17 to 26, wherein said memory comprise one or more of an EEPROM, a flash memory device, and a flash memory device emulating an EEPROM.

28. Method according to one of claims 17 to 27, wherein said memory comprises a memory chip having electrical contacts for being connected with a circuit board that are arranged such that said electrical contacts are covered by said memory chip when said memory chip is mounted on said circuit board.

29. Method according to claim 28, wherein said electrical contacts are provided in a ball-grid-array.

30. A medium readable by a data processing device, having a program recorded thereon, where the program is to make the data processing device execute the method of one of claims 17 to 29.

Abstract

Device for processing data, comprising processing means (1) for executing program routines, and memory means (2) for storing program routines to be executed by said processing means (1), where at least a part of said memory means (2) is arranged as a protected part (21) from which data can be read but which is protected against being written into, and said processing means (1) is arranged to necessarily execute a program routine stored in said protected part of said memory means upon start-up.

Fig. 1

FIG.1
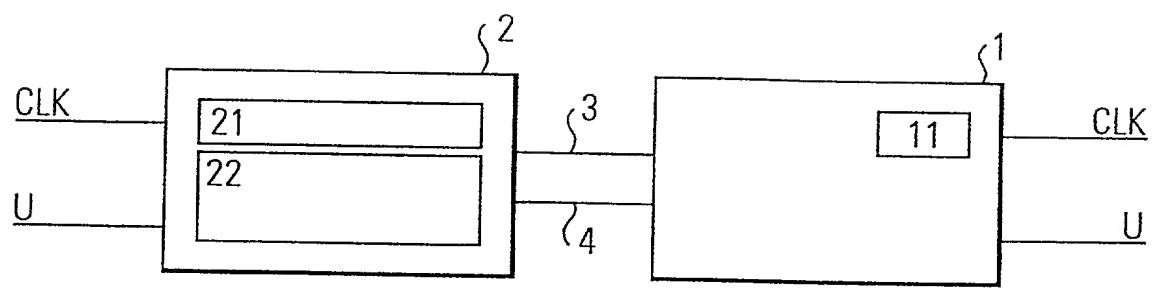
FIG.2
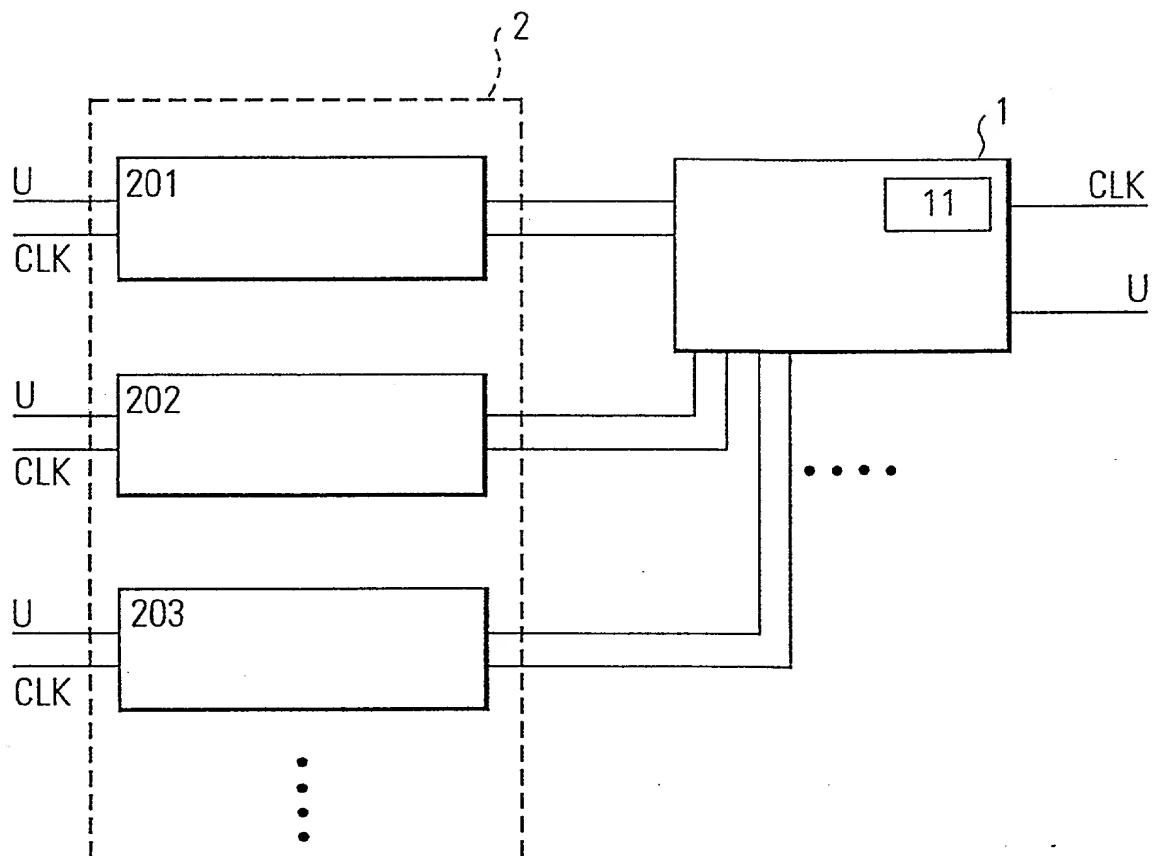
FIG.3a
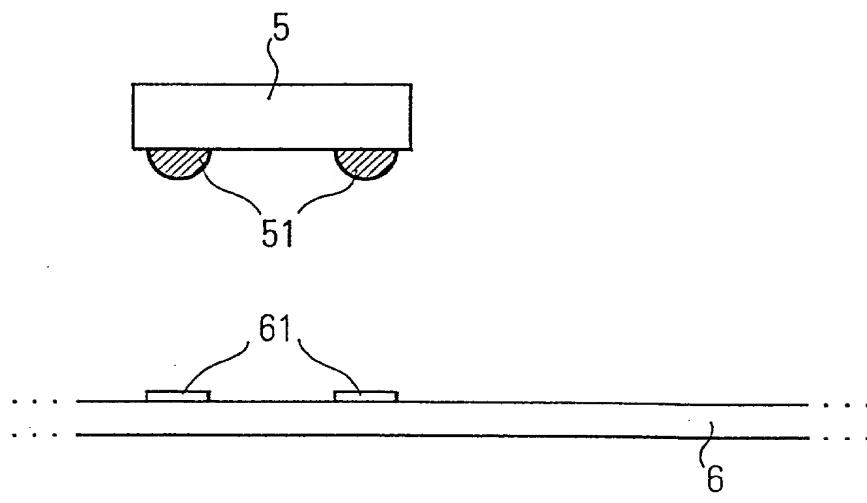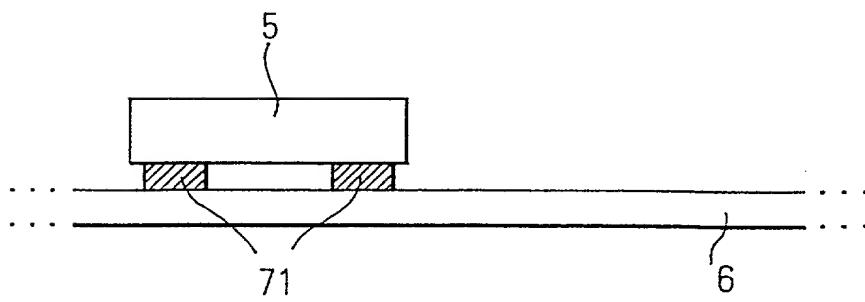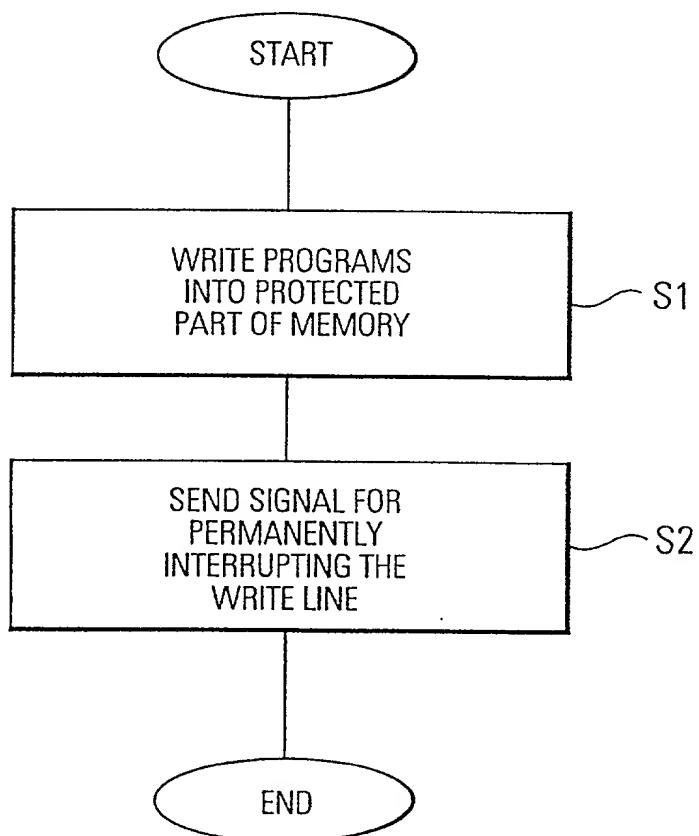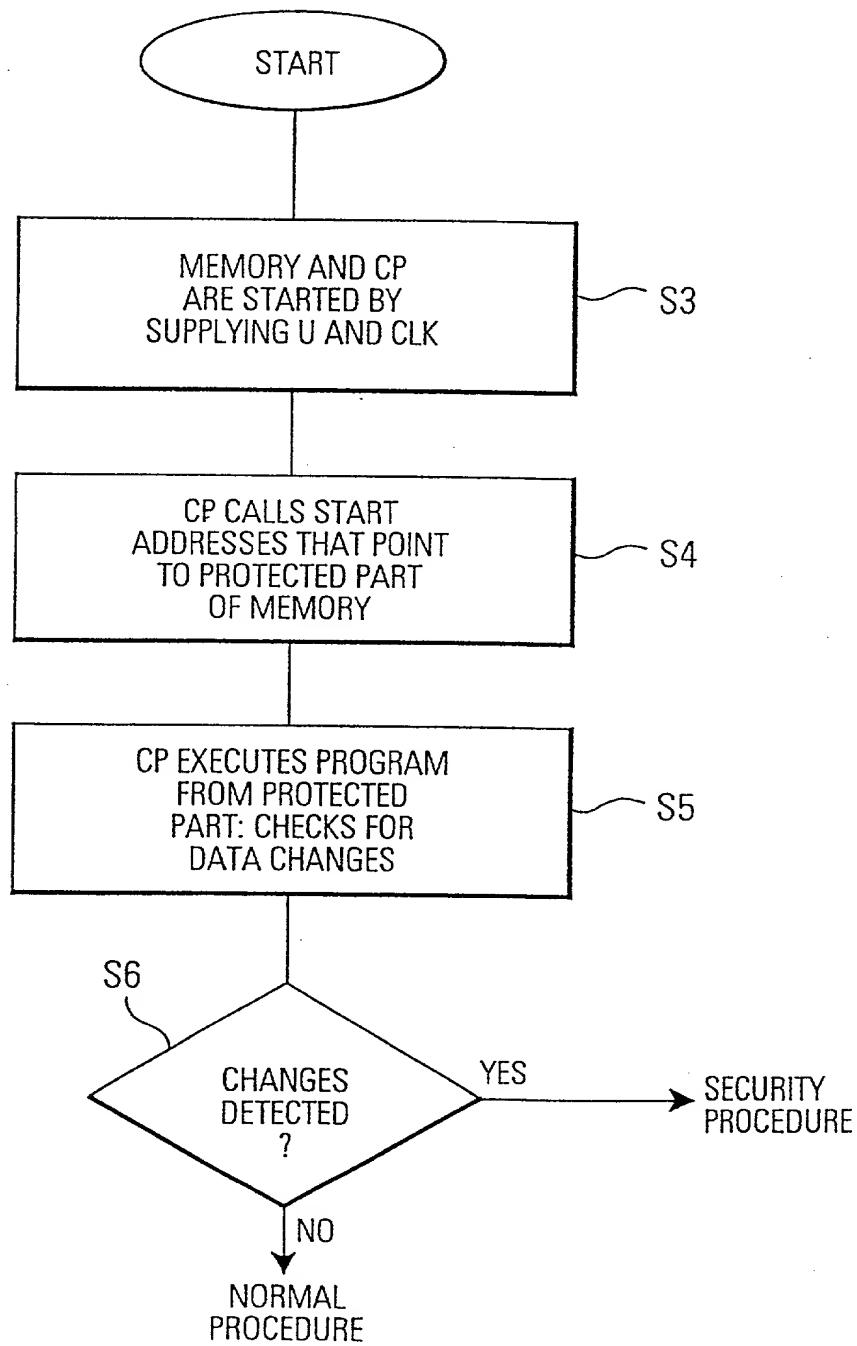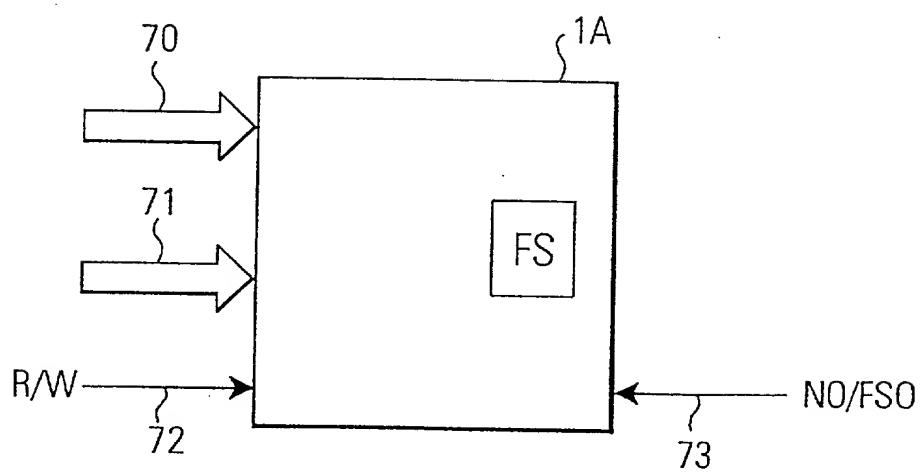
5

51

61

6

FIG.3b

5

71

6

FIG.4

```
          ┌─────────────┐
          │    START    │
          └──────┬──────┘
                 │
      ┌──────────┴──────────┐
      │   WRITE PROGRAMS    │
      │    INTO PROTECTED   │── S1
      │   PART OF MEMORY    │
      └──────────┬──────────┘
                 │
      ┌──────────┴──────────┐
      │   SEND SIGNAL FOR   │
      │    PERMANENTLY      │── S2
      │  INTERRUPTING THE   │
      │     WRITE LINE      │
      └──────────┬──────────┘
                 │
          ┌──────┴──────┐
          │     END     │
          └─────────────┘
```

FIG.5

```
              ┌─────────────┐
             (    START      )
              └──────┬──────┘
                     │
        ┌────────────┴────────────┐
        │   MEMORY AND CP          │
        │   ARE STARTED BY         │──── S3
        │   SUPPLYING U AND CLK    │
        └────────────┬────────────┘
                     │
        ┌────────────┴────────────┐
        │   CP CALLS START         │
        │   ADDRESSES THAT POINT   │──── S4
        │   TO PROTECTED PART      │
        │   OF MEMORY              │
        └────────────┬────────────┘
                     │
        ┌────────────┴────────────┐
        │   CP EXECUTES PROGRAM    │
        │   FROM PROTECTED         │──── S5
        │   PART: CHECKS FOR       │
        │   DATA CHANGES           │
        └────────────┬────────────┘
                     │
    S6           ◇───┴───◇
              ◇   CHANGES   ◇   YES        SECURITY
              ◇   DETECTED   ◇───────────► PROCEDURE
              ◇     ?       ◇
                  ◇───┬───◇
                      │ NO
                      ▼
                  NORMAL
                  PROCEDURE
```

FIG.6

RULE 63 (37 C.F.R. 1.63)
DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

As a below named inventor, I hereby declare that my residence, post office address and citizenship are as stated below next to my name, and I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

<u>Device for processing data and corresponding method</u>

the specification of which (check applicable box(s)):

☒ is attached hereto

☐ was filed on _____ as U.S. Application Serial No. _____ (Atty Dkt. No. _____

☐ was filed as PCT International application No. _____ on _____

and (if applicable to U.S. or PCT application) was amended on _____

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with 37 C.F.R. 1.56. I hereby claim foreign priority benefits under 35 U.S.C. 119/365 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed or, if no priority is claimed, before the filing date of this application:

Priority Foreign Application(s):

Application Number	Country	Day/Month/Year Fil
99 111 962.9	EP	25/06/99

I hereby claim the benefit under 35 U.S.C. §119(e) of any United States provisional application(s) listed below.

Application Number	Date/Month/Year Filed

I hereby claim the benefit under 35 U.S.C. 120/365 of all prior United States and PCT international applications listed above or below and, insofar as the subject matter of each of the claims of this application is not disclosed in such prior applications in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose material information as defined in 37 C.F.R. 1.56 which occurred between the filing date of the prior applications and the national or PCT international filing date of this application:

Prior U.S./PCT Application(s):

Application Serial No.	Day/Month/Year Filed	Status: patent, pending, abandon

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon. And I hereby appoint NIXON & VANDERHYE P.C., 1100 North Glebe Rd., 8th Floor, Arlington, VA 22201-4714, telephone number (703) 816-4000 (to whom all communications are to be directed), and the following attorneys thereof (of the same address) individually and collectively my attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith and with the resulting patent: Arthur R. Crawford, 25327; Larry S. Nixon, 25640; Robert A. Vanderhye, 27076; James T. Hosmer, 30184; Robert W. Faris, 31352; Richard G. Besha, 22770; Mark E. Nusbaum, 32348; Michael J. Keenan, 32108; Bryan H. Davidson, 30251; Stanley C. Spooner, 27393; Leonard C. Mitchard, 29009; Duane M. Byers, 33383; Jeffry H. Nelson, 30481; John R. Lastova, 33149; H. Warren Burnam, Jr. 2936; Thomas E. Byrne, 32205; Mary J. Wilson, 32955; J. Scott Davidson, 33489; Alan M. Kagen, 36178; Robert A. Molan, 29834; B. J. Sadoff, 36663; James D. Berquist, 34776; Updeep S. Gill, 37334; Michael J. Shea, 34725; Donald L. Jackson, 41090; Michelle N. Lester, 32331; Frank P. Presta, 19828; Joseph S. Presta, 35329.*

1. Inventor's Signature: _____ Date: 07.06. 00

Inventor: Bernd Möller _____ German
          (first)   MI   (last)   (citizenship)
Residence: (city) Weiherwiesen 1 _____ (state/country) Germany
Post Office Address: D-90559 Burgthann
(Zip Code) D-90559 Burgthann .7

2. Inventor's Signature: _____ Date: 7.6. 00

Inventor: Harro Osthoff _____ German
          (first)   MI   (last)   (citizenship)
Residence: (city) Ziegelsteinstrasse 189 (state/country) Germany
Post Office Address: D-90411 Nürnberg
(Zip Code) D-90411 Nürnberg

3. Inventor's Signature: _____ Date: 14.6.00

Inventor: Ben Smeets _____ Dutch
          (first)   MI   (last)   (citizenship)
Residence: (city) Dalbackavägen 11 (state/country) Sweden
Post Office Address: S-240 10 Dalby
(Zip Code) S-240 10 Dalby

FOR ADDITIONAL INVENTORS, check box ☒ and attach sheet with same information and signature and date for each.

RULE 63 (37 C.F.R. 1.63)
DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Nixon & Vanderhye P.C. (12/9?

Page 2
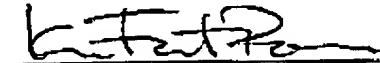
4.   Inventor's Signature:
     Inventor: Date:
          Kar-Fat Poon   British
               (first)   MI   (last)   Sweden   (citizenship)
     Residence: (city)   Mellan-Grevie 2   (state/country)
     Post Office Address: S-235 99 Vellinge
          (Zip Code)   S-235 99 Vellinge
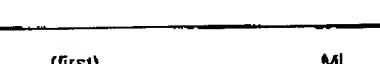
5.   Inventor's Signature: Date:
     Inventor:
               (first)   MI   (last)   (citizenship)
     Residence: (city)   (state/country)
     Post Office Address:
          (Zip Code)

6.   Inventor's Signature: Date:
     Inventor:
               (first)   MI   (last)   (citizenship)
     Residence: (city)   (state/country)
     Post Office Address:
          (Zip Code)

7.   Inventor's Signature: Date:
     Inventor:
               (first)   MI   (last)   (citizenship)
     Residence: (city)   (state/country)
     Post Office Address:
          (Zip Code)

8.   Inventor's Signature: Date:
     Inventor:
               (first)   MI   (last)   (citizenship)
     Residence: (city)   (state/country)
     Post Office Address:
          (Zip Code)

9.   Inventor's Signature: Date:
     Inventor:
               (first)   MI   (last)   (citizenship)
     Residence: (city)   (state/country)
     Post Office Address:
          (Zip Code)

10. Inventor's Signature: Date:
     Inventor:
               (first)   MI   (last)   (citizenship)
     Residence: (city)   (state/country)
     Post Office Address:
          (Zip Code)
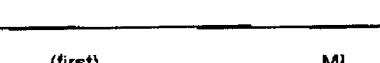
11. Inventor's Signature: Date:
     Inventor:
               (first)   MI   (last)   (citizenship)
     Residence: (city)   (state/country)
     Post Office Address:
          (Zip Code)

12. Inventor's Signature: Date:
     Inventor:
               (first)   MI   (last)   (citizenship)
     Residence: (city)   (state/country)
     Post Office Address:
          (Zip Code)